RUSSELL W. SCHRADER
Senior Vice President and
Assistant General Counsel

VISA
WORLDWIDE PARTNER

April 23, 2003

By Hand Delivery

Federal Trade Commission
Office of the Secretary
Room 159
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Re: Technology Workshop—Comment, PO34808

Ladies and Gentlemen:

This comment letter is submitted on behalf of Visa in response to the Federal Trade Commission's ("FTC") notice announcing two public workshops on May 14, 2003 and June 4, 2003 concerning the role of technology in helping consumers and businesses protect personal information. Visa supports the FTC's decision to hold the workshops and the FTC's efforts to explore measures aimed at enhancing the security of personal information available to both consumers and businesses. Visa appreciates the opportunity to comment on technology developments designed to assist consumers and businesses in securing personal information, as well as to comment on specific questions set forth in the *Federal Register* notice announcing the workshops.

The Visa Payment System, of which Visa U.S.A.[1] is a part, is the largest consumer payment system, and the leading consumer e-commerce payment system, in the world, with more volume than all other major payment cards combined. There are more than one billion Visa-branded cards, and they are accepted at more than 24 million physical locations in more than 130 countries. Visa plays a pivotal role in advancing new payment products and technologies, including technology initiatives for protecting personal information, to benefit its 21,000 member financial institutions and their hundreds of millions of cardholders worldwide.

A. General Comments on the Role of Technology in Helping Consumers and Businesses Protect Personal Information

Consumers today are increasingly using the Internet and increasingly providing information to merchants online. Consumers have expressed concern that the account

[1] Visa U.S.A. is a membership organization comprised of U.S. financial institutions licensed to use the Visa service marks in connection with payment systems.

VISA U.S.A. INC.
Post Office Box 194607
San Francisco, CA 94119-4607
U.S.A.
Phone 415 932 2178
Fax 415 932 2525

information they provide to merchants during online transactions might not be sufficiently secure. As a result, some consumers lack confidence in Internet transactions. In addition, consumers are growing more concerned about the risk of identity theft. Further, a recent survey of e-commerce executives indicated that 76 percent of those surveyed were concerned about the security of consumer credit card information. And, 50 percent of the e-commerce executives surveyed believed online credit card fraud will not go away or decline because criminals will always be working to find weaknesses in any system and exploit those weaknesses.

Visa believes that e-commerce holds the potential for increased productivity and an accompanying rise in standards of living. Visa also has a keen interest in this issue because Visa payment cards play a key role in e-commerce. However, Visa is concerned that the growth of e-commerce may be hampered by consumer concerns about information security and the potential for fraud, including identity theft. Accordingly, Visa has implemented various technologies designed to enhance the security of personal information and has identified measures consumers can take to assist in the security of their personal information.

Visa has extensive experience with the use of technology in managing information practices and in providing security for the personal information maintained. Visa has made great strides in efforts to enhance the use of technology to protect personal information and to control fraud. As a result, fraud as a percentage of Visa's total volume has declined over time, and fraudulent use of Visa payment cards presently is at an all-time low. In the late 1980s, fraud accounted for approximately 0.20 percent of the total Visa card volume; in the early 1990s, it was about 0.15 percent of total card volume; and today, fraud only accounts for 0.07 percent of total card volume.

It is in the interests of Visa, its members, their merchants, and consumers alike to protect information and to prevent and combat fraud. In addition to fostering the effectiveness of new technologies such as the Internet, fraud prevention protects merchants from bearing the costs of fraud and protects consumers from the higher prices that they would have to pay in order to cover fraud losses. Fraud prevention also protects consumers from the trouble of having to exercise their rights in connection with unauthorized transactions. For these and other reasons, fraud prevention is essential to protecting the integrity of the Visa brand name and maintaining the confidence of consumers and merchants that use the Visa system.

B. The Consumer Experience

Consumer caution about providing personal information over the Internet because of concern about the possibility of fraud and identity theft, and consumer awareness that they need to assist in the protection of their personal information or decrease their activity of e-commerce transactions, have lead consumers to seek effective measures to help in their efforts. Visa has continued to offer several means—technologies and educational

information—by which consumers can obtain additional protection, reassuring consumers that the likelihood of fraud and identity theft are diminished.

1. Technologies for Protecting Personal Information

Visa has implemented a program, Verified by Visa, that is designed to assist consumers and Internet merchants manage the risks of fraud. The overall objective of Verified by Visa is to improve the security of e-commerce payment transactions and to reduce operational expense. Verified by Visa helps prevent unauthorized use of Visa cards, providing consumers added confidence when shopping online. Specifically, Verified by Visa provides an extra precaution consumers can take to prevent unauthorized use of their cards. Consumers can register for personalized passwords through the Visa member bank that issued the consumer's card or at the Visa Web site. After creating their passwords, Visa cardholders are prompted for their passwords when shopping online at participating e-commerce merchants. Verified by Visa enables participating card issuers to validate a cardholder's identity through the use of a password during the consumer's online checkout process, while the cardholder is still at the e-commerce merchant's site.

Verified by Visa provides significant benefits to consumers, as well as to merchants and issuers. For example, consumers have the much-needed reassurance that at participating online stores they have increased protection against unauthorized use of their Visa cards. Importantly, Visa research indicates that 76 percent of consumers stated they believe online merchants should implement Verified by Visa. In addition, merchants get chargeback protection, which in turn, results in fewer issues and reduced costs associated with resolving consumer disputes. Verified by Visa also enables issuers to offer a value-added service that can increase shopping and assist retention.

2. Practical Steps to Protect Personal Information

In addition to the technologies employed by Visa designed to give merchants and consumers added security of personal information, Visa also believes that there are certain steps consumers can and should take to reduce their own security risks. For several years, Visa has continued to pursue awareness and educational initiatives, including an initiative that provides consumers with information on how to protect their cardholder information online. In particular, Visa's Web site provides "Online Security Tips" for consumers, which include the following suggestions for how consumers can shop safely on the Internet:

- Be selective when providing personal information—never give out personal or account information to anyone you do not trust.
- Look for signs of security. Symbols like an unbroken lock or key or a URL that begins https:// indicate that only you and your merchant can view your payment information.

- Never send payment information via e-mail. Information that travels over the Internet in an unencrypted manner (like e-mail) is not completely protected from being read by outside parties.
- Maintain records of your online purchases.

Visa's Web site contains links to additional sites that also serve as helpful resources for consumers. For example, Visa's Web site has a link to the Internet Security Alliance ("ISA"), of which Visa is a member. The ISA provides guidance for home computer users, describing nine actions for every home user to better secure their home computers. Visa's Web site also has a link to the Better Business Bureau's BBB*OnLine* Reliability Program ("BBB*OnLine*"), of which Visa is a member. The BBB*OnLine* Web site lists participants of the program, so that consumers may locate companies that are members of their local Better Business Bureau and that pledge to meet the BBB*OnLine* standards for ethical online business practices.

C. The Business Experience

Just as consumers must take steps to protect themselves, it is critical that businesses take the appropriate measures to protect personal information. Providing adequate security protection for both merchants and consumers is essential for the long-term success of e-commerce. Visa continues to implement several programs designed to manage information practices and enhance online security. Visa and its member financial institutions have developed a variety of security programs that help merchants further reduce the unauthorized use of Visa payment cards. These programs have a significant role in preventing and combating Internet fraud and identity theft. The Visa programs include, among others, the Cardholder Information Security Program ("CISP").

Visa's program establishing security requirements for cardholder data, CISP, defines a standard of due care and enforcement for protecting sensitive information. Currently, CISP applies to any e-commerce entity, *i.e.*, merchant or service provider, that stores or transmits Visa cardholder information. The initial effort of CISP includes an active program to ensure annual validation of selected e-merchants' security positions. All e-commerce merchants and service providers must comply with 12 basic CISP requirements, the "Digital Dozen," outlining a "best practices" approach, which include the following:

- Install and maintain a working firewall to protect data;
- Keep security patches up-to-date;
- Protect stored data;
- Encrypt data sent across public networks;

- Use and regularly update anti-virus software;
- Restrict access by "need to know";
- Assign a unique ID to each person with computer access;
- Do not use vendor-supplied defaults for passwords and security parameters;
- Track all access to data by unique ID;
- Regularly test security systems and processes;
- Implement and maintain an information security policy; and
- Restrict physical access to data.

CISP compliance with the Digital Dozen is scaled to a level of risk that is based on the number of accounts stored or processed by an e-commerce entity. For example, for select merchants and service providers that handle large volumes of cardholder information, CISP compliance assessment and monitoring occur through annual on-site reviews. For other merchants, compliance occurs through completion of an online compliance questionnaire and monthly confidential vulnerability scans. There are currently five distinct groups of CISP participants, ranging from a "select merchant" to a "compromised entity." Regardless of size, all e-commerce merchants and service providers must comply with the Digital Dozen. After a CISP assessment, Visa permits a remediation period to correct any identified weaknesses. The duration of this remediation period depends on the severity of the problem. Merchants and their service providers must meet the CISP requirements in order to continue to accept Visa Payment products. Failure to comply with the CISP requirements could result in fines, restrictions on the merchant, or permanent prohibition of the merchant or service provider's participation in Visa programs.

* * * *

Again, Visa appreciates the opportunity to comment on this important topic. If you have any questions concerning these comments, or if we may otherwise assist you further, please do not hesitate to contact me at (415) 932-2178.

Sincerely,

Russell W. Schrader
Senior Vice President and
Assistant General Counsel